

The TCP 3-way handshake works like this:

```
Client -----SYN-----> Server
Client <---ACK/SYN----- Server
Client -----ACK-----> Server
```

Why not just this?

```
Client -----SYN-----> Server
Client <-----ACK----- Server
```

A repeater is a two-port network device that regenerates the signal over a network before it becomes weak or gets damaged.

BRIDGE



A bridge is a device that joins any two networks or host segments together.

MODEM



Modems are devices that transform digital signals into the form of analog signals that are of various frequencies



ACCESS POINT

An AP or Access Point is a wireless appliance that operates on the OSI model's second layer. It can be used in two ways.

@techjockey.com

services, requirements for investigation types, and securing the provision of resources.

Diff between authentication and authorization

Authentication and authorization are two vital information security processes that administrators use to protect systems and information.

Authentication verifies the identity of a user or service
Authorization determines their access rights

Authentication

Authorization

After an employee successfully authenticates, n determines what information the employees d to access



What is the main domain you are working in cyber Security ?

TWOB



Security Operations

Security operations pertain to the tasks that put security plans into action. It covers applying resource protection techniques, disaster recovery, incident management, managing physical security, and understanding and supporting investigations.

NETWORK SWITCH



Switches play a more important role than hubs. A switch is a multi-port device that enhances network efficiency.

GATEWAY



As the name suggests, the gateway is a passage that interlinks two networks together.

Example: Employees in a company are required to authenticate through the network before accessing their company email

Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

[Malware](#) is a general term that encompasses all software designed to do harm

[Viruses](#) can be spread from one computer to another inside files. For the virus to be activated, someone has to trigger it with an external action. For example, a virus can be embedded inside a spreadsheet. If you download the spreadsheet, your computer will not necessarily be infected. The virus gets activated once you open the spreadsheet.

With a [worm](#), there is no need for the victim to open up any files or even click on anything. The worm can both run and spread itself to other computers.

What is difference between WAF and firewall?

Network firewalls cover the traffic on the network; WAFs cover the app. Using an NGFW and a WAF together gives you broader coverage. A network firewall can help stop an attack at the edge of the network by blocking incoming malicious traffic, which can benefit an application to an extent

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app

A proxy server is a system or router that provides a gateway between users and the internet.

CVE- common vulnerabilities and exposure

An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident

SIEM-

EDR-Endpoint Detection and Response

XDR-Extended Detection and Response (XDR)

UEBA-User and entity behavior analytics

Gurukul UEBA uses algorithms and machine learning to detect anomalies in the behavior of users and non-human entities such as the routers, servers, endpoints, and other devices in a network. UEBA looks for unusual or suspicious behavior that deviates from a baseline of normal everyday patterns or usage.

CASB-

EDR vs XDR

The number of endpoints continues to increase across organizations. The increase in remote work has also increased the need to secure and monitor various endpoints and endpoint-to-endpoint connections across the entire environment.

an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

EDR - Detection, investigation, and response technology that collects security-relevant data from endpoints, performs anomaly detection, enables analysts to investigate from collected telemetry, and we investigate to find the root cause of the investigation and based on that we decide further action to remediate / blocking / whitelisting etc.

XDR-

XDR (extended detection and response) **collects and automatically correlates data across multiple security layers - email, endpoint, server, cloud workload, and network**

T&T

Tactics describe the technical objectives an attacker is trying to achieve while techniques describe how an attacker achieves their objective

Webservers:

web server is **to store, process, and deliver requested information or webpages to end users**

Internet Information Services (IIS) for Windows® Server is a flexible, secure and manageable Web server for hosting anything on the Web..

CVE

1. CVE-2020-1472 (ZeroLogon)

The MS-NRPC (**Netlogon Remote Protocol**) protocol of Microsoft Windows has a vulnerability called **CVE-2020-1472, found in 2020. Stealing a user's password hash and using it as authentication enables attackers to carry out "pass-the-hash" attacks, which lets them gain unauthorized access to a network.** The potential for a hacker to access a network without the user's knowledge or assistance is what qualifies this vulnerability as a critical bug impacting millions.

2. CVE-2021-44228 (Log4Shell)

Log4j RCE (CVE-2021-44228)

The Apache Log4j 2 library for logging error messages in Java applications contains a vulnerability called Log4shell. If

successfully exploited, the vulnerability identified as CVE-2021-44228 could give **a remote hacker complete control of a device over the Internet**. Hackers can use any entry point that permits data entry from external users to confirm that the vulnerability is present and can be exploited.

These components include input fields, user and password login forms, and HTTP headers like User-Agent, X-Forwarded-For, or other unique headers. More specifically, successful Log4Shell exploration can activate the remote code execution mode, which enables an attacker to download and run a malicious payload on the server. This vulnerability has a CVSS score of 10 out of 10.

3. CVE-2022-22536 (ICMAD)

SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53, and SAP Web Dispatcher are vulnerable⁴.

4. CVE-2021-26855 (ProxyLogon)

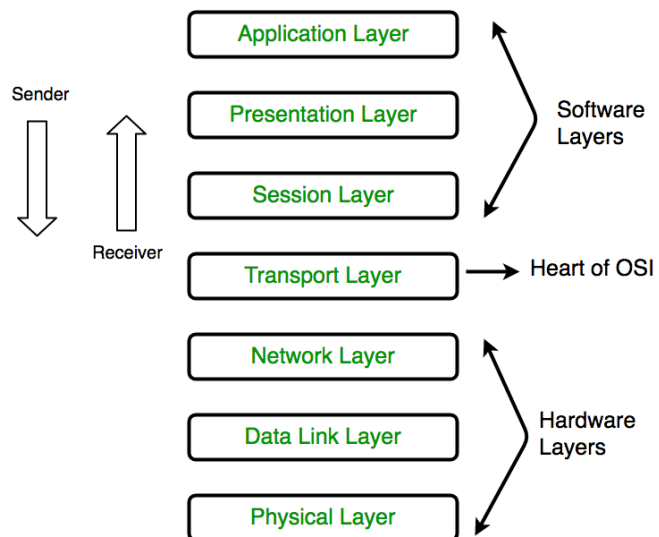
Next on any hackers list of vulnerabilities is CVE-2021-26855 discovered in Microsoft Exchange in 2021. This enables an attacker to run code remotely on a weak server, potentially gaining access to the system without authorization. Microsoft released a fix soon after the vulnerability was identified in March 2021. If you are using a vulnerable version of Microsoft Exchange Server, it is vital to ensure that you have applied the appropriate patches to protect against this vulnerability.

Hackers can easily take advantage of this vulnerability in Microsoft Exchange Server by accessing port 433 on the server without any action required from the user. To smuggling and merge requests. At the victim's request, an unauthorized attacker can deliver any data. This allows an attacker to pose as a victim or compromise an intermediary web cache. System confidentiality, integrity, and availability could all be lost entirely in the event of a successful attack. This vulnerability has a CVSS3 score of 10 out of 10.

5. CVE-2022-22965 (Spring4Shell)

Text4shell (CVE-2022-42889)

Applications using Spring MVC or Spring WebFlux and running on JDK 9+ could be exposed to remote code execution (RCE) through data binding



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

P DNT SPA

OSI model:

OSI stands for Open Systems Interconnection

Networking protocols

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network

DHCP : Dynamic host configuration protocol DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network

FTP:File transfer protocol- File Transfer Protocol enables file sharing between hosts

HTTP:Hyper text transfer protocol- **HTTP** is a TCP/IP based communication **protocol**, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web

Telnet: Telnet is an application layer protocol that enables a user to communicate with a remote device.

SNMP:Simple mail

DNS :domain naming system protocol- he DNS protocol helps in translating or mapping host names to IP addresses

SMTP☹️**Simple Mail transfer protocol**) SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side

IMAP:Internet message access protocol-IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device

POP3-The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client

Port Numbers

A port is a virtual point where network connections start and end.

Ports 20 and 21: File Transfer Protocol (FTP)

Port 22: Secure Shell (SSH)

[Port 25](#): Historically, [Simple Mail Transfer Protocol \(SMTP\)](#). SMTP is used for [email](#).

Port 53: [Domain Name System \(DNS\)](#).

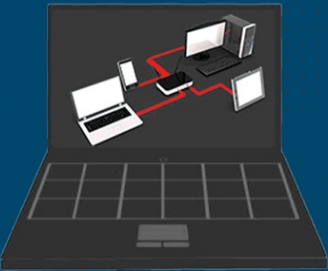
Port 80: Hypertext Transfer Protocol (HTTP).

Port 443: [HTTP Secure \(HTTPS\)](#). HTTPS is the secure and encrypted version of HTTP

Port 3389: [Remote Desktop Protocol](#) (RDP).

Networking devices

TYPES OF NETWORK DEVICES



REPEATER



A repeater is a two-port network device that regenerates the signal over a network before it becomes weak or gets damaged.

BRIDGE



A bridge is a device that joins any two networks or host segments together.

MODEM



Modems are devices that transform digital signals into the form of analog signals that are of various frequencies

ACCESS POINT



An AP or Access Point is a wireless appliance that operates on the OSI model's second layer. It can be used in two ways.

NETWORK HUB



A network hub is a multiport repeater that connects multiple wires from different branches.

NETWORK SWITCH



Switches play a more important role than hubs. A switch is a multi-port device that enhances network efficiency.

GATEWAY



As the name suggests, the gateway is a passage that interlinks two networks together.

@techjockey.com

What is IP packet ?

An IP packet is a unit of data in a network that contains **information about the source and destination addresses** and **other control information** needed to transport the packet over a network.

What is Threat, Risk, Vulnerability, Exploit, Payload ?

First, a vulnerability exposes your organization to threats. A threat is a malicious or

negative event that takes advantage of a vulnerability. Finally, the risk is the **potential for loss and damage** when the threat does occur.

Ex Vulnerability---**password is vulnerable for dictionary or exhaustive key attacks** – Threat---An intruder can exploit the password weakness to break into the system – Risk---the resources within the system are prone for illegal access/modify/damage by the intruder

What is CIA ?

- **Confidentiality** makes sure that only authorized personnel are given access or permission to modify data
- **Integrity** helps maintain the trustworthiness of data by having it in the correct state and immune to any improper modifications
- **Availability** means that the authorized users should be able to access data whenever required

What is AAA ?

Authentication verifies the identity of a user or service
Authorization determines their access rights

Authentication	Authorization
Example: Employees in a company are required to authenticate through the network before accessing their company email	Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

Accounting –

It provides means of monitoring and capturing the events done by the user while accessing the network resources

What is Data Encryption and types of Encryption ?

Data encryption is a way of translating data from plaintext (unencrypted) to ciphertext (encrypted). Users can access encrypted data with an encryption key and decrypted data with a decryption key

Asymmetric encryption, also known as Public-Key Cryptography, encrypts and decrypts the data using two separate cryptographic asymmetric keys. These two keys are known as a “public key” and a “private key” ex RSA, PKI

Symmetric encryption is a type of encryption where only one secret symmetric key is used to encrypt the plaintext and decrypt the ciphertext. Ex AES DES 3AES

What is hashing and types of hashes ?

Hashing is a one-way function that turns a file or string of text into a unique digest of the message.

What is Proxy server and types of proxy server ?

What is VPN ?

VPN stands for virtual private network. In basic terms, a VPN **provides an encrypted server and hides your IP address from corporations, government agencies and would-be hackers**. A VPN protects your identity even if you are using public or shared Wi-Fi, and your data will be kept private

What is IDS and IPS ?

An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action.

An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident

What is Active Directory ?

Active Directory (AD) is **a database and set of services that connect users with the network resources they need to get their work done**.

What is DLP (Data loss prevention) ?

What is Domain Controller ?

What is DMZ (Demilitarized Zone) ?

The main objective of a DMZ is to enable organizations to use the public internet while ensuring the security of their private networks or LANs

Servers that offer services to the public (e.g. Web servers, SMTP servers) are placed in the DMZ, while servers that offer services to internal users reside on the private network.

Common http methods

Common http response codes*

Responses are grouped in five classes:

- Informational responses (100 - 199)
- Successful responses (200 - 299)
- Redirection messages (300 - 399)
- Client error responses (400 - 499)

- Server error responses (500 - 599)

HTTP Status Code 200 - OK. ... - successful communication

- HTTP Status Code 301 - Permanent Redirect. ...
- HTTP Status Code 302 - Temporary Redirect. ...
- HTTP Status Code 404 - Not Found. ...
- HTTP Status Code 410 - Gone. ...
- HTTP Status Code 500 - Internal Server Error. ...
- HTTP Status Code 503 - Service Unavailable.
-

Common application layer attacks

What is Firewall and its types ?

What is SIEM ?

SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities

In short, SIEM gives organizations visibility into activity within their network so they can respond swiftly to potential cyberattacks and meet compliance requirements. All the traffic flowing inside the network is logged into the SIEM with its event name, time, log source, etc. data.

What is EDR ?

Common Brute force attacks

What is a Brute Force Attack?

- A brute force attack uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

Dictionary Attacks: An advanced method where a hacker uses a premade list of phrases based on research of the target or slight variations of common (or potential) passwords to run against a specific username. The list they choose to use is considered a "dictionary" of amended or slightly altered words or character combinations.

- **Reverse Brute Force Attacks:** A method where a hacker starts with a known password, either acquired from a breach or commonly used, then searches and attempts many usernames until a combination is found. Different

from a traditional brute force or dictionary attack because they are working backwards and starting with the known passwords instead of known usernames.

- **Credential Stuffing:** A method where a hacker already has known username and password combinations for one system and uses those same credentials to access other accounts, profiles, or systems associated with the same user. This attack works because users frequently recycle passwords across their accounts.

Windows Security event ids

What is Two way handshake and Three way handshake

3 way : Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

The TCP 3-way handshake works like this:

```
} Client -----SYN-----> Server
  Client <---ACK/SYN----- Server
  Client -----ACK-----> Server
```

Why not just this?

```
Client -----SYN-----> Server
Client <-----ACK----- Server
```

TCP's three-way handshake has two important functions. It makes sure that both sides know that they are ready to transfer data and it also allows both sides to agree on the initial sequence numbers,

What is Phishing email

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on fraudulent websites that pretend to be legitimate

What is Qradar Architecture

What is Cyber Kill chain

What is Encoding and Decoding ? Types of encoding method

How to prevent DOS and DDOS?

DDoS Protection Techniques

1 Reduce Attack Surface Area-

We want to ensure that we do not expose our application or resources to ports, protocols or applications. Thus, minimizing the possible points of attack

2 Deploy Firewall

use a [Web Application Firewall \(WAF\)](#) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit a vulnerability in your application itself.

Common malware attacks;

1) Adware

Adware — commonly called “spam” — serves unwanted or malicious advertising. While relatively harmless, it can be irritating as adware can hamper your computer’s performance. In addition, these ads may lead users to download more harmful types of malware inadvertently. To defend against adware, make sure you keep your operating system, web browser, and email clients updated so they can block known adware attacks before they are able to download and install.

[Malware](#) is a general term that encompasses all software designed to do harm

[Viruses](#) can be spread from one computer to another inside files. For the virus to be activated, someone has to trigger it with an external action. For example, a virus can be embedded inside a spreadsheet. If you download the spreadsheet, your computer will not necessarily be infected. The virus gets activated once you open the spreadsheet.

With a [worm](#), there is no need for the victim to open up any files or even click on anything. The worm can both run and spread itself to other computers.

[A trojan program](#) pretends to be a legitimate one, but it is in fact malicious. A trojan can't spread by itself like a virus or worm, but instead must be executed by its victim, often through social engineering tactics such as phishing.

6) Bots

A bot is a software program that performs an automated task without requiring any interaction

for example, you can add CAPTCHAs to your forms to prevent bots from overwhelming your site with requests

ransomware attacks encrypt a device's data and holds it for ransom. If the ransom isn't paid by a certain deadline, the threat actor threatens to delete or release the valuable data (often opting to sell it on the dark web).

8) Spyware

Cybercriminals use spyware to monitor the activities of users.

Example Keylogger...monitors key strokes

A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the [handshake](#). Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

SQL injection prevention:

Primary Defenses:

Option 1: Use of Prepared Statements (with Parameterized Queries)

Option 2: Use of Properly Constructed Stored Procedures

Option 3: Allow-list Input Validation

OWASP to 10

The Open Web Application Security Project (OWASP) is a nonprofit foundation dedicated to improving software security

1. Broken access control-
2. Cryptographic failures-breakdown in cryptography
3. Injection-sql injection
4. Insecure design
5. Security misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data integrity failures

9. Security logging and monitoring failures

10. Server side request forgery (SSRF)

new vulnerabilities:

- **Insecure design:** This category contains risks related to design and infrastructure flaws. Differentiated from other vulnerabilities, insecure design cannot be fixed through proper implementation.
- **Software and data entry failures:** This category includes risks related to accepting software updates without verifying integrity. This vulnerability focuses on the assumption these updates can always be trusted.
- **Server-side request forgery (SSRF):** Risks related to URL fetching from one application to another, at the user's request, without verifying the URL's integrity are grouped under this category. This server-side vulnerability is considered risky because forged requests can bypass security measures such as firewalls, VPNs, or other access controls.

latest threats:

vulnerability on cloud- misconfiguration,

mobile attacks

remote work -public wifi networks

sophisticated phishing

The main difference between IPv4 and IPv6 is **the address size of IP addresses**.

The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address